REPORT 20-13

SECURING THE EMERGING TECHNOLOGIES OF AUTONOMOUS AND CONNECTED VEHICLES

Shahab Tayeb, PhD
Matin Pirouz, PhD

April 2020

A publication of
Mineta Transportation Institute
Created by Congress in 1991

College of Business
San José State University
San José, CA 95192-0219

TECHNICAL REPORT DOCUMENTATION PAGE

1. Report No. 20-13	**2. Government Accession No.**	**3. Recipient's Catalog No.**
4. Title and Subtitle Securing the Emerging Technologies of Autonomous and Connected Vehicles		**5. Report Date** April 2020 **6. Performing Organization Code**
7. Authors Shahab Tayeb, PhD, https://orcid.org/0000-0002-7466-1042 Matin Pirouz, PhD, https://orcid.org/0000-0002-6255-4741		**8. Performing Organization Report** CA-MTI-1915
9. Performing Organization Name and Address Mineta Transportation Institute College of Business San José State University San José, CA 95192-0219		**10. Work Unit No.** **11. Contract or Grant No.** ZSB12017-SJAUX
12. Sponsoring Agency Name and Address State of California SB1 2017/2018 Trustees of the California State University Sponsored Programs Administration 401 Golden Shore, 5th Floor Long Beach, CA 90802		**13. Type of Report and Period Covered** Final Report **14. Sponsoring Agency Code**

15. Supplemental Notes

DOI: 10.31979/mti.2020.1915

16. Abstract

The Internet of Vehicles (IoV) aims to establish a network of autonomous and connected vehicles that communicate with one another through facilitation led by road-side units (RSUs) and a central trust authority (TA). Messages must be efficiently and securely disseminated to conserve resources and preserve network security. Currently, research in this area lacks consensus about security schemes and methods of disseminating messages. Furthermore, a current deficiency of information regarding resource optimization prevents further efficient development of this network. This paper takes an interdisciplinary approach to these issues by merging both cybersecurity and data science to optimize and secure the network. The proposed method is to apply Prim's algorithm to an existing vehicular security scheme, Privacy-Preserving Dual Authentication Scheme (PPDAS), to further network efficiency in terms of power and time consumption. When a dual authentication security scheme is in place, the time taken for message dissemination follows a quadratic growth; applying Prim's algorithm to the security scheme reduces the time to disseminate messages to a linear growth. The number of messages sent was decreased by a magnitude of up to 44.57. Contemporary security schemes are compared with PPDAS to justify the overhead consumption. Through the proposed approach, the usage of network resources, such as power and time, is reduced, which substantially enhances the performance of the vehicular network and allows for the scalability of the IoV.

17. Key Words Vehicular ad hoc networks, Network resources, Internetworking, Data analysis	**18. Distribution Statement** No restrictions. This document is available to the public through The National Technical Information Service, Springfield, VA 22161		
19. Security Classif. (of this report) Unclassified	**20. Security Classif. (of this page)** Unclassified	**21. No. of Pages** 16	**22. Price**

Form DOT F 1700.7 (8-72)

DOI:
10.31979/mti.2020.1915

Mineta Transportation Institute
College of Business
San José State University
San José, CA 95192-0219

Tel: (408) 924-7560
Fax: (408) 924-7565
Email: mineta-institute@sjsu.edu

transweb.sjsu.edu

ACKNOWLEDGMENTS

The authors thank Editing Press, for editorial services, as well as MTI staff, including Executive Director Karen Philbrick, PhD; Deputy Executive Director Hilary Nixon, PhD; Graphic Designer Alverina Eka Weinardy; and Executive Administrative Assistant Jill Carter.

TABLE OF CONTENTS

LIST OF FIGURES

EXECUTIVE SUMMARY

With the proliferation of support for autonomous and connected vehicles in private and public sectors, many Cyber-Physical Systems (CPS) of different types, sizes, and sensitivity levels exist. The framework developed herein would be applicable to new and existing CPS, resulting in a more secure physical and virtual network of autonomous and connected vehicles. Autonomous and connected vehicles are increasingly gaining momentum across different disciplines, but the lack of standards and models for their design and implementation are major barriers ahead of such research and development, particularly from a security perspective. The project's proposed framework would act as a baseline to facilitate security testing and assessment of a given vehicular network which paves the way for the development of advanced security analytics tools, leading to new knowledge discoveries in this area. The security of such networks is a fertile field and establishing a framework to make such networks secure would certainly trigger many interdisciplinary scholarly activities. The proposed research is an original and systematic investigation of security, and is potentially transformative in nature as it challenges conventional wisdom in the field.

Smart objects and smart embedded sensors are currently secured based on the same best practices as traditional networks without considering the limitations imposed by the proliferation of smart nodes in terms of processing power and memory. This is mainly due to limited research in this field. Encapsulation of protocol stack layers is done on a single hardware processor, leaving the lower layers unprotected. With so many new forms of data, new forms of threats would come into existence. The main reasons for CPS security breaches are: i) Conventional network security wisdom is not applicable to the IoT realm. IoT is an ecosystem driven by business gaps, rather than just a myriad of devices; ii) IoT vendors compromise security to gain functionality and openness for a broader target market. IoT manufacturers follow Agile manifesto for their development process which opens many security gaps; iii) There are inherent vulnerabilities in individual IoT nodes: a) For many types of IoT devices, physical access cannot be restricted, and thus devices that expose critical information on internal nodes can be compromised; b) Although chip manufacturing innovations have led to the emergence of embedded chips with hardware-based security (e.g. ARM TrustZone) and hardware with cryptography support (e.g. ARMv8), the inclusion of such chips in every device is cost prohibitive. Thus, it makes sense to look for network security solutions that do not require modification of existing and emerging IoT devices; and c) IoT nodes generally don't support advanced networking capabilities and security protocols.

I. INTRODUCTION

Intelligent Transportation Systems (ITSs) aim to provide a safe and efficient transportation system by establishing a large network that enables vehicles to communicate with one another and with road-side base units.[1] ITS alleviates traffic congestion, load-balances traffic, and holds records to further the efficiency of network use. Analyses of various events throughout the network (e.g., failures due to car malfunction) are performed to adapt to users' needs.[2] The government, research community, and society need the ITS to be safe, reliable, and dependable.[3] An international standard on the engineering of security for autonomous vehicles is in development, demonstrating the vitality of a stable vehicular network.[4]

For ITS to be actualized, there needs to be interconnectivity between transportation units.[5] The Internet of Vehicles (IoV) conceptualizes vehicles and road-side units connecting and communicating through purely IP-based infrastructure.[6] The IoV requires the system to foster communications between vehicles; messages may include a vehicle's identification number, speed, or coordinates. The transmission of these messages must be secure,[7] calling for a security scheme in the network.[8]

If message dissemination is not optimized, it would lead to network overloading, which can compromise the network's functionality.[9] IoV nodes run on limited resources, and if communication is not optimized, resources would be misused and nodes would run overtime. The slowing of the network can lead to increased power consumption, which in turn leads to increased costs which might compromise economic feasibility. Extensive traffic also takes resources that could be allocated to security. This deficiency in resources leaves the network vulnerable to attacks such as Denial of Service,[10] man-in-the-middle,[11] and replay attacks.[12]

II. RELATED WORK

OPTIMIZATION OF MESSAGE DISSEMINATION

Congestion in a vehicular network causes slowing of the network and packet drops. In order to prevent network congestion, network flooding of messages needs to be avoided. One such approach is to prevent vehicles from forwarding messages that have already been received.[13]

POWER CONSUMPTION

Cybersecurity-related power consumption is a necessary consideration when developing the IoV. Resources are constrained, so the most cost-effective energy management decisions must be made while maintaining safety and functionality.[14] Since the IoV would face more physical exposure, security mechanisms must be robust, yet lightweight and efficient.[15] The various power management research can be categorized as centralized energy management by direct optimization of power signals or decentralized energy management through indirect optimization and management of power signals (often done through an intermediary).[16] All of the techniques, however, aim to minimize power consumption to optimize the network; the above requirements have been accounted for when selecting a security scheme to analyze in this report.

III. METHODS

SELECTION OF PRIM'S ALGORITHM

Prim's algorithm is commonly used as a method to shorten and optimize message paths. The time complexity for Prim's algorithm, which is O(E log(V)), where E is the number of edges in the graph and V is the number of vertices in the graph, is efficient. While there are other MST algorithms, the time complexities are less efficient than Prim's. For example, Bellman-Ford's algorithm has a time complexity of O(MN), where N is the number of nodes in the graph and M is the number of edges in the graph. With this second order time complexity for Bellman-Ford's algorithm, Prim's algorithm would be a better alternative when it comes to decreasing the number of packets.

SELECTION OF PPDAS SECURITY SCHEME

Privacy-Preserving Dual Authentication Scheme (PPDAS) provides a strong privacy-preservation method, low bandwidth consumption, and minimal key management requirements. The security design also utilizes a variety of elements from other security methods and introduces the use of trust evaluation within the processes.

IV. RESULTS AND PERFORMANCE

Three simulations were run to test for different traffic densities with different numbers of vehicles, each for 300 seconds at a four-way-intersection stoplight.

TIME ANALYSIS

Figure 1 and Figure 2 highlight the benefits of using a MST to reduce the time to disseminate a message to the entire network. Using Prim's algorithm keeps network congestion and packet loss significantly lower than flooding the network.

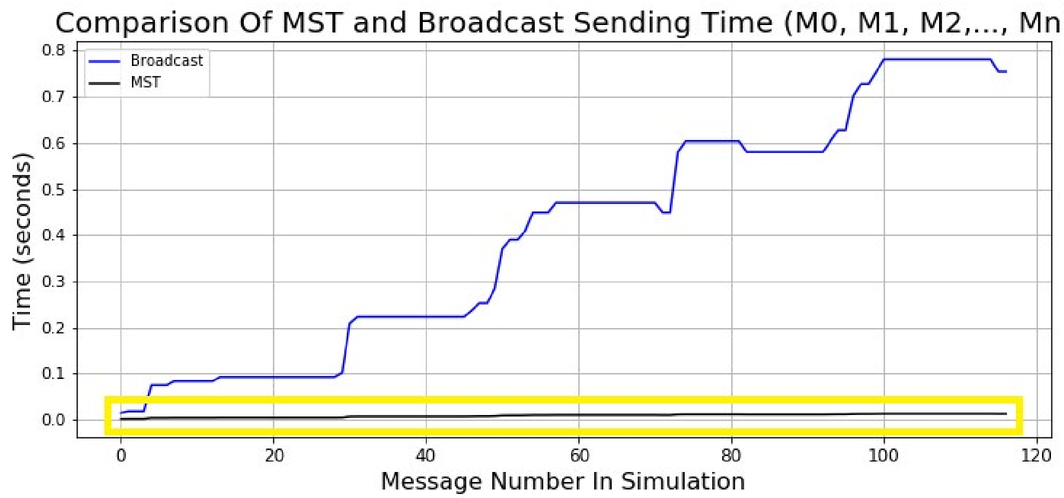

Figure 1. Time of Prim's and Flooding Disseminating a Message to the Entire Network (Highlighted section shown in Figure 2)

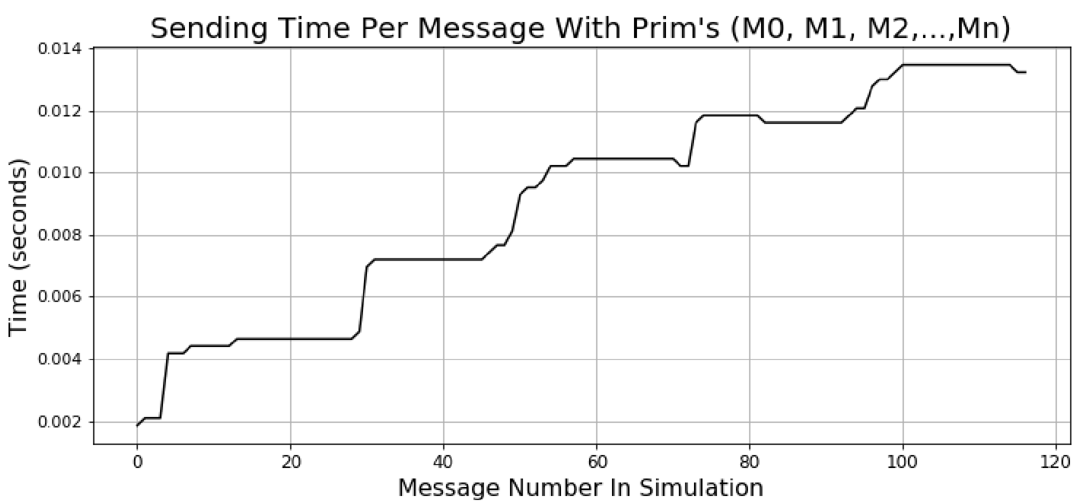

Figure 2. A Closer Look at Using Prim's to Disseminate Messages to the Entire Network

Figure 3 shows the time for each algorithm to disseminate messages throughout the entire network as the number of vehicles increases. Flooding the network appears to have a quadratic time growth, while Prim's algorithm has a linear growth.

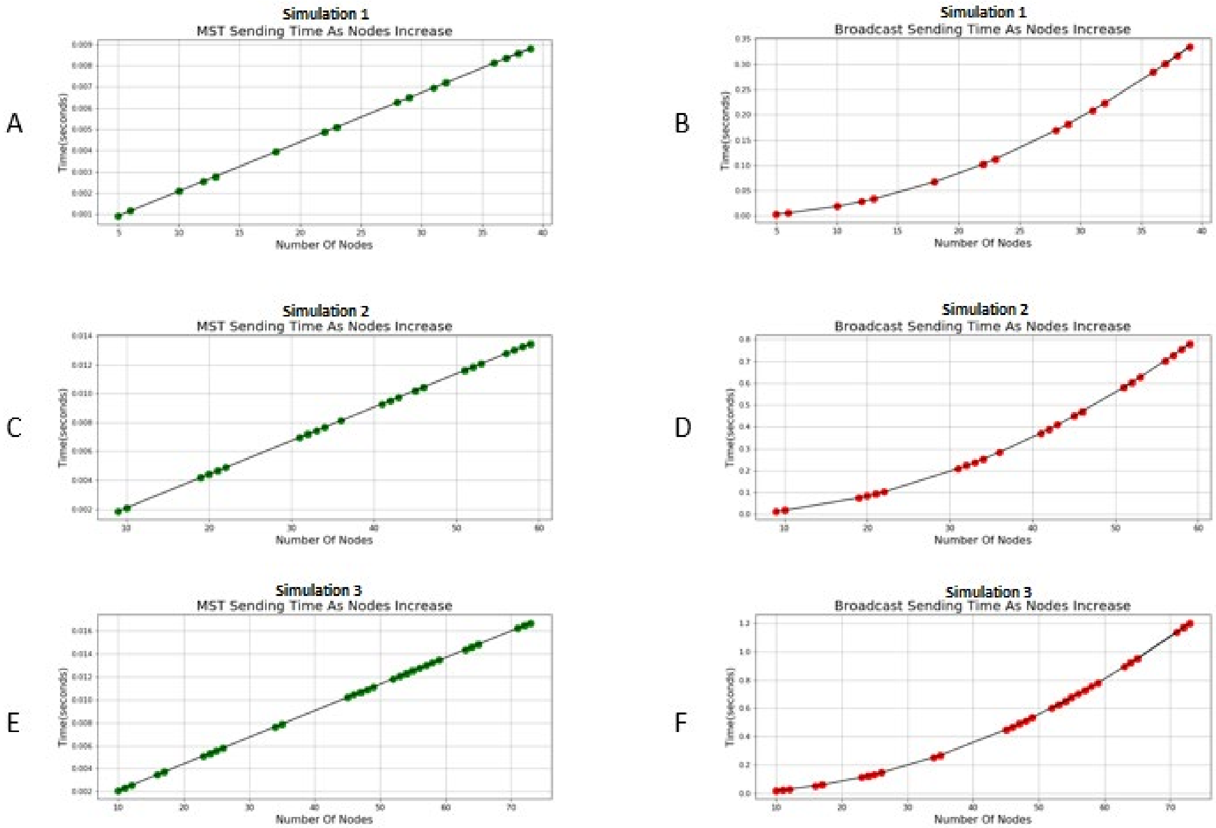

Figure 3. Graphs Depicting Time to Disseminate Messages as Number of Vehicles Increases with Prim's Algorithm and Broadcasting

The time spent disseminating messages by flooding the network is 47.12 seconds; Prim's algorithm reduced that time to 1.05 seconds. Simulations one, two, and three had time savings of magnitudes 28.06, 44.56, and 53.88 respectively.

In Figure 4, the extra overhead is applied for several different authentication security schemes. The focus of this security analysis is on PPDAS. The total sending time without any security scheme applied is 1.057 seconds, and with PPDAS applied, it is 1.104 seconds, increasing overhead by 4.45%.

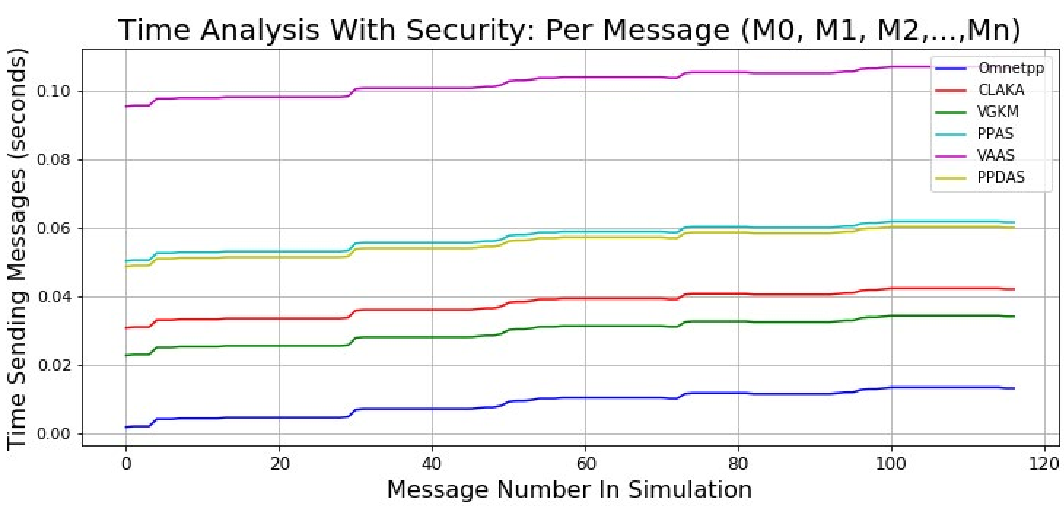

Figure 4. Time Analysis of the Security Schemes Applied to Sent Messages

POWER ANALYSIS

Figure 5 and Figure 6 show the relationship between vehicles in the network and power consumed. Using MST, it takes 0.012 Watts to disseminate a message; using flooding, it takes 0.673 Watts, saving power by a magnitude of 56.08.

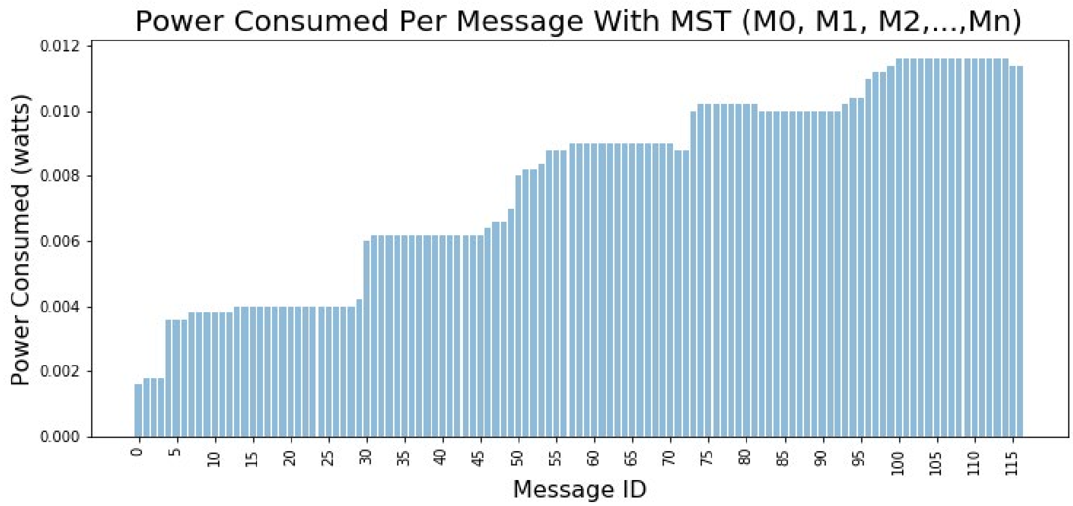

Figure 5. The Amount of Power used to Disseminate Each Message using Prim's Algorithm

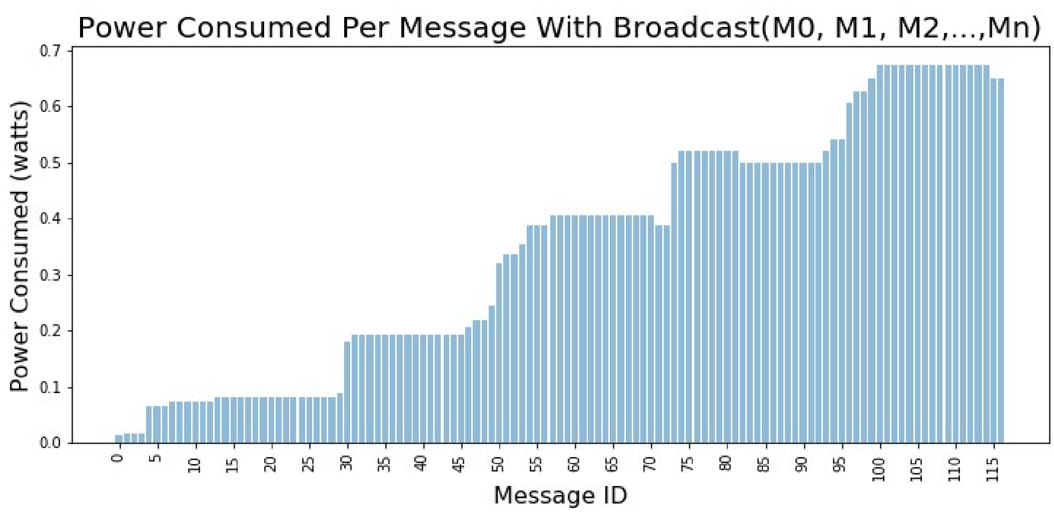

Figure 6. The Amount of Power used to Disseminate Each Message by Flooding the Network

Figure 7 shows the power savings of Prim's versus flooding for disseminating messages throughout the entire network.

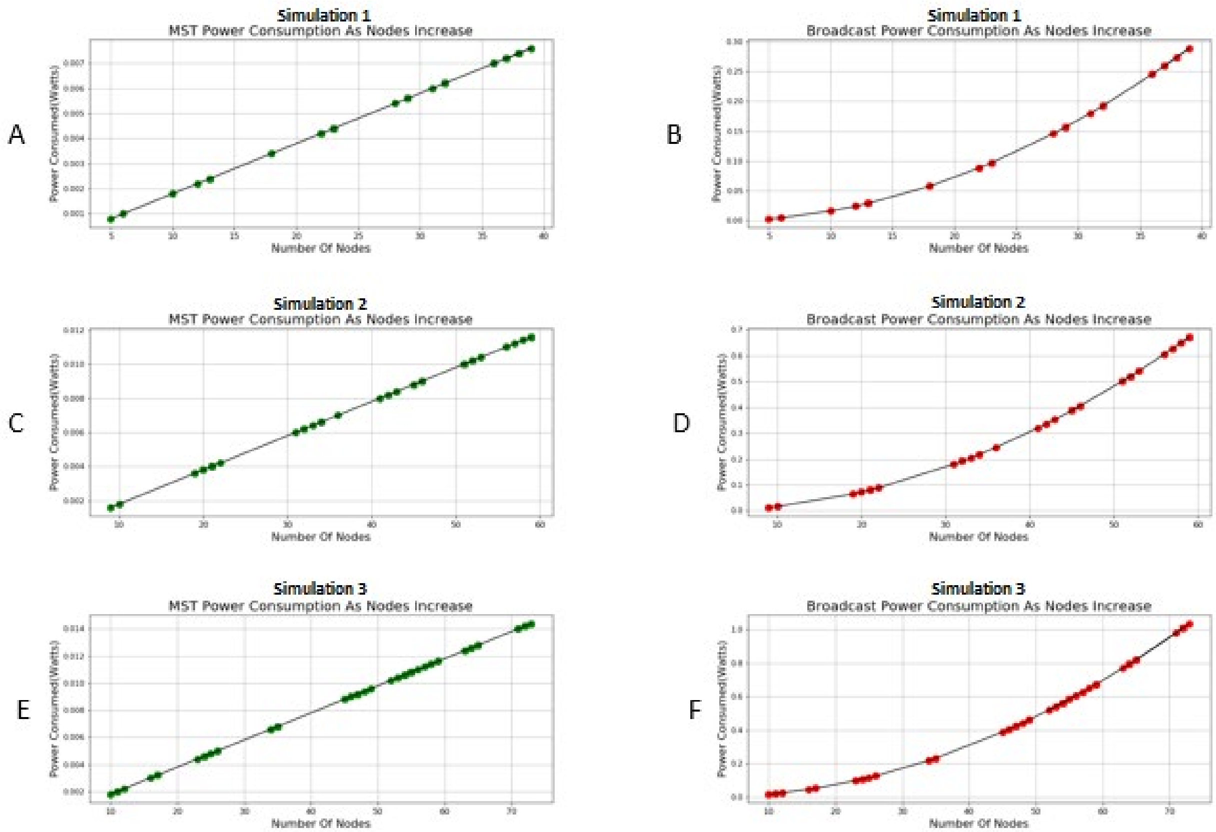

Figure 7. Power Required to Disseminate Messages as the Number of Vehicles Increases using Prim's and Broadcast

Figure 8 shows the power consumption of Prim's and flooding. The total power consumed in simulation two using flooding is 40.62 Watts, and using Prim's it is 0.91 Watts. Simulation experiments one, two, and three had savings in power by magnitudes of 28.06, 44.57, and 53.88, respectively.

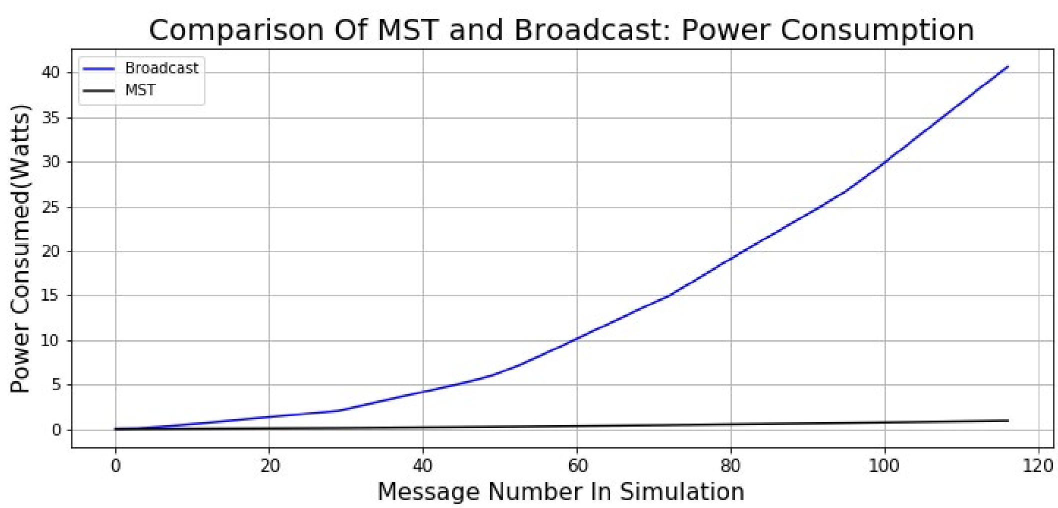

Figure 8. An Analysis of the Total Power Consumed Disseminating Messages with Flooding and Prim's

V. CONCLUSION

This paper takes an interdisciplinary approach and couples data science and cybersecurity to tame message dissemination in the IoV. Prim's algorithm is applied to various vehicular security schemes and is analyzed to justify the selection of PPDAS to work in conjunction with the selected MST algorithm. A comparative analysis of the proposed method against broadcast techniques for message dissemination is conducted. The simulation demonstrated the proposed method provides a decrease in time taken to disseminate messages and a reduction in power consumption. The increase in efficiency in vehicular communication allows for more resources to be dedicated to other features for the IoV. Future research prospects include power consumption analysis as it applies to different protocols, analyzing how to optimize power consumed per message as it travels various distances in the network, and a multi-hop re-authentication protocol for message dissemination.

ABBREVIATIONS AND ACRONYMS

CLAKA	Certificateless Key Agreement Scheme
IoV	Internet of Vehicles
ITS	Intelligent Transportation Systems
IoV	Internet of Vehicles
OBU	On-Board Unit
PPDAS	Privacy-Preserving Dual Authentication Scheme
RSU	Road-Side Unit
TA	Trust Authority
VAAS	Vehicular Anonymous Authentication Scheme
VANET	Vehicular Ad-Hoc Network
VGKM	Vehicular Group Key management
WSN	Wireless Sensor Network

ENDNOTES

1. George Dimitrakopoulos, "Intelligent Transportation Systems Based on Internet-Connected Vehicles: Fundamental Research Areas and Challenges," *11th International Conference on ITS Telecommunications,* 2011. https://doi.org/10.1109/itst.2011.6060042.

2. Gennady Andrienko et al., "Visual Analytics of Mobility and Transportation: State of the Art and Further Research Directions," *IEEE Transactions on Intelligent Transportation Systems* 18 (2017): 2232–49. https://doi.org/10.1109/tits.2017.2683539.

3. Juan Contreras-Castillo, Sherali Zeadally, and Juan Antonio Guerrero-Ibanez. "Internet of Vehicles: Architecture, Protocols, and Security." *IEEE Internet of Things Journal* 5 (2018): 3701–9. https://doi.org/10.1109/jiot.2017.2690902; Ivana Tomic and Julie A. Mccann, "A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols," *IEEE Internet of Things Journal* 4 (2017): 1910–23. https://doi.org/10.1109/jiot.2017.2749883; Kathy Pretz, "Internet of Things Technology Will Connect Highways, Street Lights, and Vehicles," *IEEE Spectrum*, June 2019.

4. "ISO/SAE CD 21434," *ISO,* November 2018, https://www.iso.org/standard/70918.html; Christoph Schmittner, Gerhard Griessnig, and Zhendong Ma, "Status of the Development of ISO/SAE 21434," *Communications in Computer and Information Science Systems, Software and Services Process Improvement,* 2018, 504–13, https://doi.org/10.1007/978-3-319-97925-0_43.

5. Shahab Tayeb, Matin Pirouz, and Shahram Latifi, "A Raspberry-Pi Prototype of Smart Transportation," *25th International Conference on Systems Engineering (ICSEng),* 2017, https://doi.org/10.1109/icseng.2017.25.

6. George Dimitrakopoulos, "Intelligent Transportation Systems Based on Internet-Connected Vehicles: Fundamental Research Areas and Challenges," *11th International Conference on ITS Telecommunications,* 2011, https://doi.org/10.1109/itst.2011.6060042.

7. Contreras-Castillo, Juan, Sherali Zeadally, and Juan Antonio Guerrero-Ibanez, "Internet of Vehicles: Architecture, Protocols, and Security," *IEEE Internet of Things Journal* 5 (2018): 3701–9, https://doi.org/10.1109/jiot.2017.2690902.

8. Jamil K. Naufal et al., "A2CPS: A Vehicle-Centric Safety Conceptual Framework for Autonomous Transport Systems," *IEEE Transactions on Intelligent Transportation Systems* 19 (2018): 1925–39, https://doi.org/10.1109/tits.2017.2745678.

9. N. Wisitpongphan et al., "Broadcast Storm Mitigation Techniques in Vehicular Ad Hoc Networks," *IEEE Wireless Communications* 14 (2007): 84–94, https://doi.org/10.1109/mwc.2007.4407231.

10. "Proceedings of the 2003 ACM Workshop on Rapid Malcode – WORM03," 2003.

11. M. Conti, N. Dragoni, and V. Lesyk, “A Survey of Man In The Middle Attacks,” *IEEE Communications Surveys Tutorials* 18 (2016): 2027–51.

12. Haowen Tan, Dongmin Choi, Pankoo Kim, Sungbum Pan, and Ilyong Chung, “Comments on ‘Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks,’” *IEEE Transactions on Intelligent Transportation Systems* 19 (2018): 2149–51, https://doi.org/10.1109/tits.2017.2746880; Ding Wang et al., “On the Challenges in Designing Identity-Based Privacy-Preserving Authentication Schemes for Mobile Devices,” *IEEE Systems Journal* 12 (2018): 916–25, https://doi.org/10.1109/jsyst.2016.2585681.

13. N. Wisitpongphan et al., “Broadcast Storm Mitigation Techniques in Vehicular Ad Hoc Networks,” *IEEE Wireless Communications* 14 (2007): 84–94, https://doi.org/10.1109/mwc.2007.4407231.

14. Ivana Tomic and Julie A. Mccann, “A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols,” *IEEE Internet of Things Journal* 4 (2017): 1910–23, https://doi.org/10.1109/jiot.2017.2749883.

15. Ivana Tomic and Julie A. Mccann, “A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols,” *IEEE Internet of Things Journal* 4 (2017): 1910–23, https://doi.org/10.1109/jiot.2017.2749883.

16. Junjie Hu, Yang Li, and Huayanran Zhou, “Energy Management Strategy for a Society of Prosumers Under the IOT Environment Considering the Network Constraints,” *IEEE Access* 7 (2019): 57760–68, https://doi.org/10.1109/access.2019.2913724.

BIBLIOGRAPHY

Andrienko, Gennady, Natalia Andrienko, Wei Chen, Ross Maciejewski, and Ye Zhao. “Visual Analytics of Mobility and Transportation: State of the Art and Further Research Directions.” *IEEE Transactions on Intelligent Transportation Systems* 18 (2017): 2232–49. https://doi.org/10.1109/tits.2017.2683539.

Conti, M., N. Dragoni, and V. Lesyk. “A Survey of Man In The Middle Attacks.” *IEEE Communications Surveys Tutorials* 18 (2016): 2027–51.

Contreras-Castillo, Juan, Sherali Zeadally, and Juan Antonio Guerrero-Ibanez. “Internet of Vehicles: Architecture, Protocols, and Security.” *IEEE Internet of Things Journal* 5 (2018): 3701–9. https://doi.org/10.1109/jiot.2017.2690902.

Dimitrakopoulos, George. “Intelligent Transportation Systems Based on Internet-Connected Vehicles: Fundamental Research Areas and Challenges.” 2011 *11th International Conference on ITS Telecommunications,* 2011. https://doi.org/10.1109/itst.2011.6060042.

Hu, Junjie, Yang Li, and Huayanran Zhou. “Energy Management Strategy for a Society of Prosumers Under the IOT Environment Considering the Network Constraints.” *IEEE Access* 7 (2019): 57760–68. https://doi.org/10.1109/access.2019.2913724.

“ISO/SAE CD 21434.” *ISO,* November 2018. https://www.iso.org/standard/70918.html.

Naufal, Jamil K., Joao B. Camargo, Lucio F. Vismari, Jorge R. De Almeida, Caroline Molina, Rodrigo Ignacio R. Gonzalez, Rafia Inam, and Elena Fersman. “A2CPS: A Vehicle-Centric Safety Conceptual Framework for Autonomous Transport Systems.” *IEEE Transactions on Intelligent Transportation Systems* 19 (2018): 1925–39. https://doi.org/10.1109/tits.2017.2745678.

Pretz, Kathy. “Internet of Things Technology Will Connect Highways, Street Lights, and Vehicles.” *IEEE Spectrum*, June 2019.

“Proceedings of the 2003 ACM Workshop on Rapid Malcode – WORM03,” 2003. https://doi.org/10.1145/948187.

Schmittner, Christoph, Gerhard Griessnig, and Zhendong Ma. “Status of the Development of ISO/SAE 21434.” *Communications in Computer and Information Science Systems, Software and Services Process Improvement,* 2018, 504–13. https://doi.org/10.1007/978-3-319-97925-0_43.

Tan, Haowen, Dongmin Choi, Pankoo Kim, Sungbum Pan, and Ilyong Chung. “Comments on ‘Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks.’” *IEEE Transactions on Intelligent Transportation Systems* 19 (2018): 2149–51. https://doi.org/10.1109/tits.2017.2746880.

Tayeb, Shahab, Matin Pirouz, and Shahram Latifi. “A Raspberry-Pi Prototype of Smart Transportation.” *2017 25th International Conference on Systems Engineering (ICSEng)*, 2017. https://doi.org/10.1109/icseng.2017.25.

Tomic, Ivana, and Julie A. Mccann. “A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols.” *IEEE Internet of Things Journal* 4 (2017): 1910–23. https://doi.org/10.1109/jiot.2017.2749883.

Wang, Ding, Haibo Cheng, Debiao He, and Ping Wang. “On the Challenges in Designing Identity-Based Privacy-Preserving Authentication Schemes for Mobile Devices.” *IEEE Systems Journal* 12 (2018): 916–25. https://doi.org/10.1109/jsyst.2016.2585681.

Wisitpongphan, N., O.k. Tonguz, J.s. Parikh, P. Mudalige, F. Bai, and V. Sadekar. “Broadcast Storm Mitigation Techniques in Vehicular Ad Hoc Networks.” *IEEE Wireless Communications* 14 (2007): 84–94. https://doi.org/10.1109/mwc.2007.4407231.

ABOUT THE AUTHORS

DR. SHAHAB TAYEB

Dr. Shahab Tayeb is a faculty member with the Department of Electrical and Computer Engineering in the Lyles College of Engineering at California State University, Fresno. Dr. Tayeb's research expertise and interests include network security and privacy, particularly in the context of the Internet of Vehicles. His research incorporates machine learning techniques and data analytics approaches to tackle the detection of zero-day attacks. Through funding from the Fresno State Transportation Institute, his research team has been working on the security of the network backbone for Connected and Autonomous Vehicles over the past year. He has also been the recipient of several scholarships and national awards including a U.S. Congressional Commendation for STEM mentorship.

DR. MATIN PIROUZ

Dr. Matin Pirouz is a faculty member with the Department of Computer Science at California State University, Fresno. Dr. Pirouz's research current interests include CS Education, big data analytics, social network analysis, and data mining. Her current projects include applying prescriptive and descriptive analyses. Her research has been funded by the National Science Foundation and other federal, state, and private funding agencies.

PEER REVIEW

San José State University, of the California State University system, and the Mineta Transportation Institute (MTI) Board of Trustees have agreed upon a peer review process required for all research published by MTI. The purpose of the review process is to ensure that the results presented are based upon a professionally acceptable research protocol.